FMIPv6 적용을 위한 보안 아키텍처 연구

손상우*, 김문기*, 이병호*
*한양대학교 정보통신학과
e-mail : cyberscv@naver.com

A Study on Security Architecture for FMIPv6

Sang-Woo Son*, Mun-Gi Kim*, Byung-Ho Rhee*
*Dept. of Information and Commnunications, Hanyang University

요 약

FMIPv6 는 Mobile IPv6 에서의 빠른 핸드오버를 지원하기 위해 고안된 프로토콜이다. 이 프로토콜은 핸드오버시 이동할 라우터의 정보를 예측하여 Fast Binding Update(FBU)를 한다는 장점을 제공한다. 그러나, 현재 FMIPv6 프로토콜은 FBU 전송 시 이동 노드와 라우터 사이에 서로를 완벽히 신뢰할 수 없다는 문제점을 가진다. 이를 보완하기 위한 신뢰 보안기능이 요구되었다. 따라서, 본 논문에서는 FMIPv6 프로토콜을 구조적으로 보안성을 강화시킬 아키텍처를 제안하였다.

1. 서론

최근 휴대인터넷, 무선 LAN 서비스 등 무선인터넷 분야가 각광을 받고 있고, 향후 국내 IT 분야를 주도할 것으로 사료된다.

무선 인터넷의 주된 핵심은 가장 개인화 된 단말기인 이동전화 또는 PDA 등 휴대장비에서 고정된 단말기 (PC)환경과 같은 인터넷 서비스를 사용할 수 있다. 이러한 무선 인터넷 환경에서의 이동성을 지원하기 위한 핵심기술이 Mobile IP 이며, Mobile IP 기술은 차세대 인터넷 기술로 각광을 받고 있다.

Mobile IP 는 IP 주소를 가진 단말의 이동시 그 연결을 항상 보장하는 기술이다. 이것은 이원화된 주소체계를 통하여 이동성을 지원하고, 임시 주소를 이용하여 단말이 이동한 라우팅 지역이 변하는 것에 따라 지속적인 인터넷 서비스를 가능하게 하는 것이다. 이와 같은 서비스 제공을 위해 이동성을 극대화 할 수 있는 Mobile IPv6[1] 기술이 주목을 받고 있다.

Mobile IP 의 이동성 지원을 위해 이동 노드가 새로운 망으로 이동하였을 때, 빠르게 다시 연결하여 서비스를 제공하느냐에 관심을 받고 있다.

핸드오버의 딜레이를 줄이고 Fast Handovers를 지원하기 위한 방법들이 제안이 되고 있으며, 그 중 Fast Handovers for Mobile IPv6(FMIPv6)[2] 는 이동할 망의 정보를 얻어 미리 바인딩 업데이트를 수행하여 핸드오버 딜레이를 줄이는 방안이다. 이 프로토콜은 이동 경로를 예측했을 시와 이동 시의 두가지 시나리오가 있다. 첫번째 시나리오에서의 Fast Binding Update시 이 패킷이 합법적으로 이동 노드로부터 전송받은 것인지 보증하지 못한다. 이러한 문제점을 해결하기 위하여 SA(Security Association) [5]를 통한 해결 방안에 대하여 연구중에 있다. 하지만 SA 설립 과정은 절차상 딜레이를 내포하고 있어서, AR(Access Router)와 이동 노드사이에 빈번한 SA 설정은 지연 문제를 가지고있다. 또한, 이후에 새로운 망과 연결시에 CN과의 RR 과정, 패킷 포워딩 과정에서의 SA 설립과정 역시 위에서 언급한 내용과 같은 문제점이다. 두번째 시나리오에서는 핸드오버시 새로운 망의 라우터와 시그널링을 하던중에 L2 핸드오버가 이루어진 경우를 말한다. 아직 L3 핸드오버가 이뤄지지 않아 새로운 CoA를 할당받지 못한 상태이다. IPSec을 사용하지 못함으로 새로운 망의 라우터는 접근한 이동노드가 합법적인 노드인지 판단을 할 수가 없다는 문제점을 가지고 있다.[1]

본 논문에서는 위에서 언급하였던 FMIPv6 에서의

[1] 본 연구는 대학 IT연구센터 육성 지원 사업의 연구결과로써 HY-SDR 연구센터의 연구비 지원으로 수행되었음

도메인내의 효율적인 SA 설립에 관한 제안과 이동 노드와 라우터간의 인증방안에 대해서 제안했다.본 논문의 구성은 다음과 같다.

제 2 장에서는 FMIPv6 의 간단한 설명과 문제점에 대하여 기술하고, 제 3 장에서는 본 논문에서 제안하고자 하는 보안 아키텍처에 대한 세부 사항에 대해 기술한다. 제 4 장에서는 제안한 아키텍처의 결론을 맺는다.

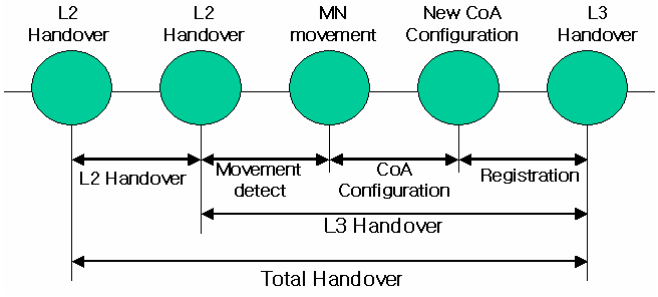
2. 관련 연구

1. FMIPv6

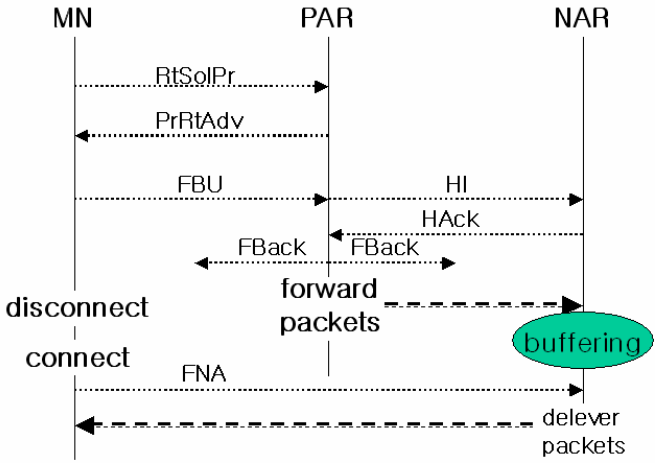
일반적인 MIPv6 환경에서의 핸드오버 과정에서는 이동성 감지(Movement Detection), 새로운 임시 주소 설정(new Care of Address configuration), 위치 정보 등록(binding update) 등의 과정을 거치며 서비스 중단 시간이 존재한다.(그림 1) 이러한 총 지연 시간은 실시간 데이터 전송이나 기타 성능에 민감한 환경에 적응하기가 어렵다. 이러한 지연 시간을 줄이기 위한 방안으로 IETF 에서는 FMIPv6 방식을 제안하였다. 이 메커니즘은 두가지 시나리오를 가진다. 동작 과정은 (그림 2)과 (그림 3)와 같다.

FMIPv6 에서는 L2 (Layer 2) 핸드오버는 기술하지 않고 L3 (Layer 3) 핸드오버에 관하여 설명하고 있다. 이동 노드는 스캐닝 과정을 통하여 현재 접속한 AP 보다 더 좋은 시그널을 받았을 경우 또는 다른 문서에서 언급한 L2 트리거에 의해 핸드오버를 예측할 수 있다. 이 예측한 결과를 가지고 L3 핸드오버를 시작한다. 이동 노드는 이동하고자 하는 새로운 액세스 라우터(nAR: New Access Router)에 대한 정보를 얻기 위해 RtSolPr (Router Solicitation for Proxy) 메시지를 현재 액세스 라우터(pAR: Previous Access Router)에게 보내고, pAR 은 이에 대한 응답으로 nAR 의 정보가 담긴 PrRtAdv (Proxy Router Advertisement) 메시지를 이동 노드에게 보낸다. 이동 노드는 pAR 에 연결된 상태에서 새로운 NCoA(New Care of Address)를 구성하고, FBU(Fast Binding Update) 메시지를 pAR 에게 보내어 곧 핸드오버가 일어날 것임을 알린다. FBU 메시지를 받은 pAR 은 NCoA 의 유효성 확인과 nAR 사이에 양방향 터널(bi-directional tunnel)을 설정하기 위하여 HI(Handover Initiation) 메시지를 nAR 로 보낸다. 이에 대한 응답으로 nAR 은 HACK(Handover Acknowledge) 메시지를 pAR 에게 전송 한다. 이 메시지를 받은 pAR 은 HACK 메시지의 상태 코드를 보고 이동 노드에 의해 요청된 핸드오버가 수락될 것인지를 검사한 다음 이에 대한 결과를 FBack 메시지에 담아 이동 노드의 이전 PCoA 로 오는 모든 패킷들을 nAR 로 포워딩하기 시작한다. 그 후 L2 핸드오버가 이뤄진 후 이동 노드는 FNA(Fast Neighbor Advertisement) 메시지를 이용하여 이동했음을 nAR 에게 알린다. 이후에 버퍼링된 패킷들이 이동 노드로 포워딩된다. 이 시나리오상에서는 FBU 를 pAR 에게 전송할 시에 전송된 노드의 주소만으로는 이동 노드를 정확히 신뢰할 수 없다. 그래서 반드시 임시적인 SA 를 이동 노드와 라우터 사이에 맺어야 한다. 하지만 빈번한 SA 설정 과정은 핸드오버 딜레이를 증가시킬 수 있다.

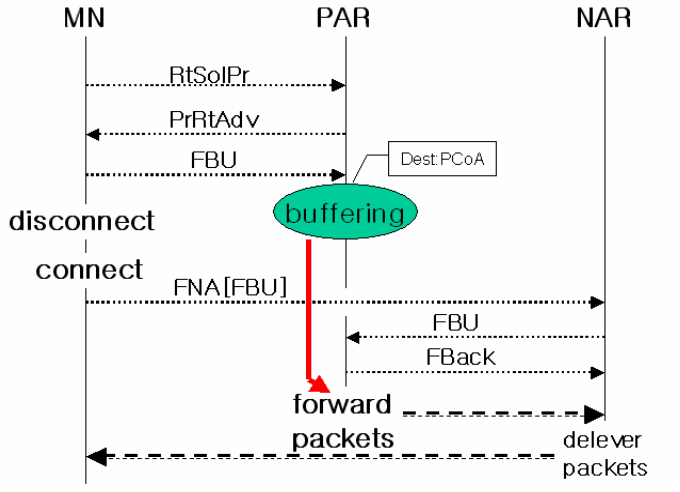
두번째 시나리오는 예측하는 상황과 FBU 전송시까지는 첫번째 시나리오와 같지만 FBack 메시지를 받아야 하는 상황에서 L2 핸드오버가 일어나서 받지 못하는 상황을 기술한다. 이 경우에 이동 노드는 L2 핸드오버가 완료되자마자 FNA 메시지안에 FBU 를 인캡슐레이션하여 nAR 에게 전송한다. NAR 은 접근한 이동 노드가 합법적인 노드 인지를 판단 할 방법은 주소를 통한 것이며, 전송된 NCoA 의 중복여부를 체크하는 방법에 의해 체크하는 방법이 유일하다.



(그림 1) MIPv6 핸드오버 과정



(그림 2) FMIPv6 첫번째 시나리오



(그림 3) FMIPv6 두번째 시나리오

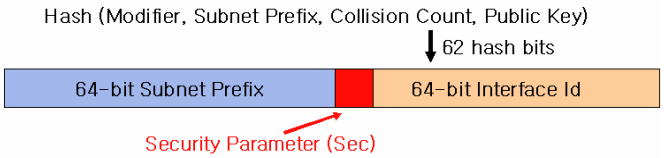
2. Cryptographically Generated Addresses

상대방과 통신상에서의 보안은 IPSec 을 사용하여 지원된다. IPSec 은 상대방과 SA 를 맺기 위하여 IKE (Internet Key Exchange)를 이용하여 키를 교환한다. ND (Neighbor Discover y)를 이용하여 IP 를 자동으로 설정할 경우, 문제가 발생한다. IKE 를 사용하기 위해서는 SA 가 필요하고, SA 를 맺기 위해서는 IP 주소가 필요하게되어 '닭이 먼저냐 달걀이 먼저냐'와 같은 문제가 발생하게 된다. 이 문제점을 해결하기 위한 방안이 CGA[3]다. CGA 는 공개키와 파라미터 값을 이용한다. 우선, 암호화된 인터페이스 식별자(interface ID)는 해쉬 계산으로 암호화하고 보안 파라미터(Sec) 적용한 후 생성된다. 해쉬 생성 알고리즘은 SHA-1 을 사용한다. 그 다음에 생성된 인터페이스 식별자와 라우터로부터 받은 서브넷 프리픽스를 합하여 암호화된 주소를 생성한다. 상대방은 받은 패킷의 정보를 토대로 해쉬 계산하여 주소를 생성한다. 생성한 결과와 일치하면 신뢰된 노드라고 판단한다. 이 CGA 의 사용은 SEND(Secure Neighbor Discovery)[4]의 CGA 옵션으로 사용이 가능하다. CGA 의 생성 속도는 보안 파라미터(Sec) 값에 따라 변하게 되며, 다음과 같다(그림 4)

시스템 / SecParam	라우터 시스템 (P4-1.6GHz)	일반노드 시스템 (Mobile P3-1133)
0	0.000045 sec	0.00011 sec
1	0.8434 sec	1.1264 sec

(그림 4) CGA 생성시 Sec 값에 따른 생성 속도

본 논문에서는 FMIPv6 에서의 두 가지 시나리오에 대한 보안성 강화를 주제로 연구하였다. 첫 번째 시나리오에서의 연구는 빈번한 SA 설정시에 걸리는 지연시간을 줄이기 위하여 Root AR 이 관리하는 지역에서의 AR 간 이동시에 빈번한 SA 를 설정을 없애고, 보안 파라미터를 재사용하여 빠른 터널을 구성하는 것이다. 두번째 시나리오에서의 연구방안은 예측 이동 전 핸드오버시에 이동 노드와 라우터간의 인증 방안이다. 채택한 방법은 CGA 를 이용한 서로간의 신뢰체인 형성에 관한 것이다.[3]



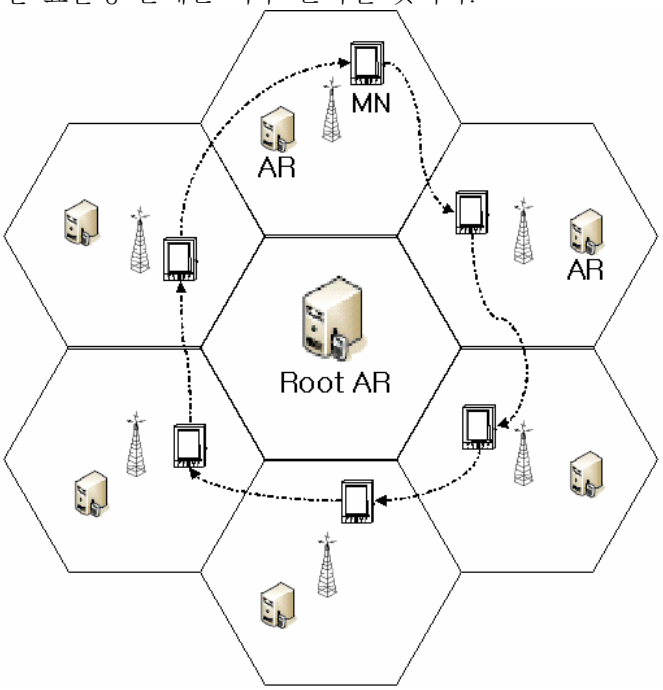
이동 노드를 신뢰하기 위한 인증 방안으로서 사용한다.

3. 제안된 보안 아키텍처 및 방법

1. 제안된 기본 아키텍처

제안된 FMIPv6 보안 아키텍처는 (그림 5)와 같다. 이 시나리오에서는 보안요소를 적용할 범위를 도메인으로 한정한다. 그리고 각 노드들은 CA 의 위임을 받은 Root Access Router(AR)로부터 인증서를 받는다. Root AR 은 도메인상에서 적용할 공개키, 알고리즘, 보안 파라미터들을 관리하게 된다. 그림에서와 같이 Root AR 이 각각 지역 셀을 관리하는 Access Router(AR)들에게 도메인상에서 사용될 보안 요소 정보들을 알려주게 되고, 보안 요소가 변경되었을 시에 재분배하게 된다. 그 후 AR 들은 받은 보안 요소를 적용하고 노드와 통신시에 사용하게 된다. 이동 노드와 AR 사이에 SA 설립 후 이동노드가 새로운 망으로 이동시에 pAR 은 nAR 로 SA 정보를 전달하게 된다. 완전한 핸드오버가 이뤄진 후에 기존 SA 설정은 파괴가 된다. 그 후 이동 노드와 nAR 은 기존의 SA 를 사용하기 위해 pAR 와 이동노드로부터 받은 SA 의 파라미터를 체크하여 일치하고, SA 의 Lifetime 이 유효하다면 SA 재사용이 허락되고, 그렇지 않으면 새로운 SA 가 성립을 시도한다. 이것은 새로이 SA 설립하지 않고 사용할 수 있다는 장점이 있습니다. 또한 이동 노드와의 통신시에 키 교환을 해야하는 부하를 줄일 수 있고, 또한 SA 설립시에 간편하게 설정이 가능하다.

이 아키텍처에서 제안한 구조에 적합한 알고리즘으로써 공개키 기반의 RSA 보안 알고리즘을 선호한다. 무선환경이라는 것을 고려하였을 때, 키의 길이는 적을수록 속도면에서 좋지만, 안정성을 고려하여 512, 768bit 등 최적화된 길이를 선택해야하며 키길이에 대한 효율성 문제는 차후 논의될 것이다.



(그림 5) Root AR 의 커버리지 영역

2. FMIPv6 에서의 적용

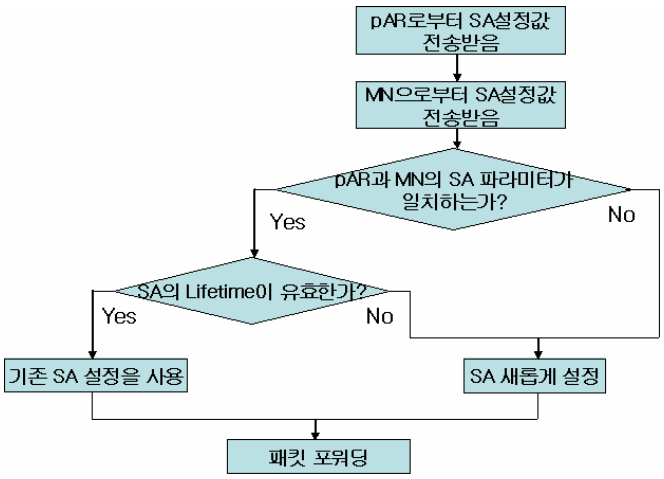
2.1 예측 이동 시나리오상의 보안 적용

위에서 제안된 구조상에서 FMIPv6 를 도입하는 시나리오를 제안한다. 이동 노드는 pAR 로부터 nAR 로 이동하려 한다고 했을 때, 우선적으로 pAR 에게 RtSolPr 메시지를 전송하여 nAR 의 정보를 요청한다. 그 후에 PrRtAdv 메시지를 이용하여 응답을 받는다.

이 과정후에 이동 노드와 pAR 사이에 서로를 인증하기 위하여 SA 가 설립되게 된다. 보안요소, 정책 등 교환없이 미리 약속되어 있는 규약으로 SA 를 맺게된다. 다른 망으로 완전히 이동하기 전에, pAR 은 nAR 로 이동 노드와의 SA 정보를 넘겨준다. 그 후 터널은 완벽히 이동 후에 파괴된다. 그리고 새로운 망에서의 노드는 기존의 SA 의 값들을 비교하여 일치한다면 재사용 할 수 있다. SA 의 설정 값과 순서도는 다음 (그림 6), (그림 7)과 같다.

```
nAR SPD OUT:
  IF source = nAR's Home Address & destination =
        MN's NCoA & proto = MH(To Be Assigned IANA)
  THEN USE SA SA2
nAR SPD IN:
  IF source = MN's NCoA & destination = nAR's Home
        Address & proto = MH(To Be Assigned IANA)
  THEN USE SA SA1
nAR SAD:
  SA2(OUT, SPI, MN's NCoA, ESP, TRANSPORT) :
  source = MN's NCoA & destination = MN's Home
  Address & proto MH
```

(그림 6) NAR 의 SA Configuration (SA2 적용시)



(그림 7) NAR 의 SA 설정 순서도

2.2 예측 이동 전 핸드오버시 보안 적용

FMIPv6 에서의 두번째 시나리오상에서의 보안상 문제점은 Binding Update 를 완료하지 않은 상태에서의 핸드오버가 일어났을 경우이다. 이동 노드는 nAR 에게 FNA 메시지를 전송한다. 하지만 이 경우에는 아직 NCoA 를 받지 않았으므로 IPSec 을 사용할 수가 없다. 그래서 이동 노드와 nAR 사이에 인증할 수가 없다. 호스트 인증 방안으로 CGA 를 채택하였다. FNA 의 CGA 옵션을 추가하여 nAR 이 전송한 노드가 합법적인 노드인지 판단을 할 수 있게 된다.

4. 결론

Mobile IPv6 의 빠른 핸드오버를 지원하기 위한 프로토콜인 FMIPv6 는 핸드오버 발생시에 이동할 새로운 망의 정보를 이동하기 전에 갖고, Fast Binding Update 를 시도하기 때문에 반드시 노드와 라우터간의 인증 절차는 필요하다.

이 논문에서는 공개키 알고리즘에 기반하여 특정 도메인 커버리지 영역안에서 이동 노드가 이동시에 기존망과의 SA 를 다른 AR 영역에서도 사용함으로써 노드를 인증하고 빠른 핸드오버를 지원할 수 있는 방안에 대하여 제안하였다. 이동 노드와 pAR 간의 SA 를 맺고 핸드오버가 일어난 후에 이 SA 정보를 nAR 에 전달하여 새로운 설정없이 다시 재사용하여 SA 설정 비용을 줄이는 방안을 제시하였다. 또한, 예측 이동 전에 핸드오버 발생시 노드와 라우터 간의 인증방안인 CGA 를 FNA 메시지에 추가함으로써 보안성을 강화한다는 추가 방안도 제시하였다.

향후, 이 도메인 안에서의 AR 와 Root AR 사이의 인증 방안과 다른 도메인 이동시에 키 교환에 대하여 연구가 필요하고, Mobile 이라는 특성을 고려한 보안키 최소화와 동일한 키사용의 횟수에 대한 논의가 요구된다.

5. 참고문헌

[1] D. Johnson, C. Perkins and J. Arkko, “Mobility Support in IPv6”, RFC3775, (2004).
[2] Koodli, R., “Fast Handovers for Mobile IPv6”, RFC4068, July 2005.
[3] Aura, T., “Cryptographically Generated Addresses (CGA)”, RFC 3972, March 2005.
[4] J. Arkko, Ed. Ericssion, J. Kemf., “Secure Neighbor Discovery (SEND)”, RFC 3971, March 2005.
[5] S.Kent, R. Atkinson., “Security Architecture for the Internet Protocol”, RFC 2401, November 1998.
[6] Jae-Wook Yu, In-Kap Park, Joong-Min Kim ., “A Study on Implementation of IPv6 Neighbor Discovery Protocol supporting Security Function), The Institude of Electronics Engineers of Korea, December 2004.
[7] J.Arkko, V.Devarapalli., “Using Ipsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”, RFC 3776, June 2004.